Richtlinie

zum Umgang mit Informationen unterschiedlicher Vertraulichkeits-klassen

Flughafen München GmbH

Version 1.7

Organisation:	**Verantwortlich:**
IT	Informationssicherheitsbeauftragter der FMG (Alexander Cmarits, Michael Schmitz)

Inhalt

1 Grundlagen zum Umgang mit Informationen

Die Flughafen München GmbH (FMG) misst dem Schutz von Informationen große Bedeutung bei, da deren Missbrauch zu großen materiellen und immateriellen Schäden führen kann. Die Klassifizierung und angemessene Handhabung von Informationen ist ein wichtiger Baustein zur Vermeidung solcher Schäden.

Informationen können in unterschiedlicher Form vorliegen – z. B. in elektronischer Form als Datei, in physischer Form als Ausdruck oder auch als gesprochenes Wort. Informationen werden anhand der Vertraulichkeit ihres Inhalts eingestuft. Der Grad der Vertraulichkeit spiegelt das Maß der Auswirkungen wider, falls Informationen missbräuchlich benutzt werden. Er bestimmt auch, wie mit Informationen umzugehen ist. Die Einstufung der Information ist unabhängig vom verwendeten Medium.

Grundsätzlich sollen nur diejenigen Personen Zugriff zu unternehmenskritischen Informationen erhalten, die diese zur Erfüllung ihrer Aufgaben benötigen.

2 Geltungsbereich

Die vorliegende Richtlinie gilt für jeden Mitarbeiter der FMG. Sie enthält nähere Bestimmungen zur Geheimhaltungspflicht jedes Mitarbeiters (s. dazu auch die Arbeitsordnung der FMG, § 5[1]).

Jeder Mitarbeiter soll im Informationsaustausch mit einer externen Stelle (z. B. Geschäftspartner) darauf hinwirken, dass auch diese die Anforderungen der Richtlinie einhält. Für die Beteiligungsgesellschaften der FMG und die dortigen Beschäftigten gilt die Richtlinie nicht unmittelbar; jeder Mitarbeiter der FMG sollte jedoch auch hier wie gegenüber externen Stellen darauf hinwirken, dass die Richtlinie eingehalten wird.

Verstöße gegen diese Richtlinie sind eine Verletzung arbeitsrechtlicher Pflichten und können entsprechende arbeitsrechtliche, zivil- und strafrechtliche Maßnahmen nach sich ziehen.

Die Richtlinie trat zum 1. Juli 2008 in Kraft.

3 Verantwortlichkeiten und Rollen

3.1 Informationsverantwortlicher

Der Informationsverantwortliche ist verantwortlich für die Klassifizierung von Informationen in seinem Verantwortungsbereich. Typischerweise gehört er der ersten oder zweiten Führungsebene an oder hat bereichsübergreifende Aufgaben (z. B. Revision, Beihilfe, IS, Arbeitsschutz, Datenschutz). Er legt den Kreis der Kernnutzer und sonstigen Nutzer (interne und ggf. externe Personen) namentlich oder über Rollen sowie deren Berechtigungen

[1] http://emotion/home1/richtlinien/mitarbeiter/verhalten/arb-ord/arbeitsordnung.pdf

fest. Bei Aufgaben- und Funktionsänderungen passt er die Berechtigungen entsprechend an. Die Verantwortlichkeit zur Klassifizierung von Informationen kann durch ihn auch an andere Mitarbeiter delegiert werden.
Für bestimmte Gruppen von Informationsnutzern, bestimmte Arten des Informationsaustauschs oder für Einzelfälle kann von dem Informationsverantwortlichen aus sachlichen Gründen von den Bestimmungen der Richtlinie abgewichen werden. Jede Abweichung muss bekannt gegeben und dokumentiert werden.

3.2 Verfasser

Der Verfasser arbeitet im Auftrag des Informationsverantwortlichen und übernimmt die Einstufung der Information von diesem. Bezüglich der Weitergabe besitzt er keine Sonderrechte.

3.3 Nutzer

Nutzer einer Information sind alle Personen, die berechtigt sind, diese Information zu erhalten. Der Nutzer handelt gemäß den Regeln dieser Richtlinie, sofern der Informationsverantwortliche nicht Abweichendes vorgegeben hat.

3.4 Kernnutzer

Kernnutzern einer Information ist der Umgang mit dieser Information vertraut; sie sind dafür entsprechend geschult und sensibilisiert. Innerhalb der Kernnutzer können Informationen ohne Rücksprache mit dem Informationsverantwortlichen weitergegeben werden. Beispiele für Kernnutzer einer Information sind die Mitarbeiter der Personalabteilung bezüglich Personalakten oder abteilungsübergreifende Projektteams – auch mit externen Beratern – bezüglich Projektdaten.

3.5 Technischer Sachbearbeiter

Technische Sachbearbeiter (z. B. Administratoren, Archivare) haben aufgrund ihrer besonderen Rolle Zugriffsmöglichkeiten auf alle Informationen. Sie sind nicht berechtigt, diese Informationen außerhalb ihrer funktionsbezogenen Aufgabe (z. B. Monitoring, Auswertung für Verrechnungszwecke) zu verwenden.

3.6 Prüfer und Ermittler

Dieser Personenkreis hat expliziten Zugriff auf Informationen zum Zwecke der Ermittlung oder Prüfung. Zum Personenkreis zählen z. B. öffentliche Regierungsstellen (Polizei, Luftamt etc.), Steuer- und Wirtschaftsprüfer, interne Revision oder Auditoren.

4 Klassifizierung von Informationen – Vertraulichkeitsklassen

4.1 Grundlagen

Alle in der FMG vorhandenen Informationen werden abhängig von ihrer Bedeutung für die Geschäftsprozesse oder dem potentiellen Schaden bei falschem Umgang mit ihnen einer der vier Vertraulichkeitsklassen **„Offen“**, **„Dienstlich“**, **„Vertraulich“** oder **„Streng vertraulich“** zugeordnet. Informationen, die auf amtliche Veranlassung geheim gehalten werden müssen (Geheimschutz), bleiben von dieser Klassifizierung unberührt.

4.2 Schadensgrößen

Für die korrekte Einstufung von Informationen in die jeweiligen Vertraulichkeitsklassen ist das Wissen um den potentiellen Schaden bei unsachgemäßem Umgang wichtig.

Schadensgröße	Schaden für das Unternehmen
Groß bis Existenz gefährdend	Betroffen ist das gesamte Unternehmen Wirtschaftliche Schäden bis zur Existenzgefährdung Geld- und Haftstrafen auf Grund von Gesetzesverstößen Erheblicher Verlust von Ansehen und Vertrauen
Mittel	Betroffen ist ein Unternehmensbereich Erheblicher wirtschaftlicher Schaden Ordnungswidrigkeiten oder Geldstrafen auf Grund von Gesetzesverstößen Imageverlust, Verärgerung einzelner Kunden
Gering	Schaden nur gering, keine weit reichenden Konsequenzen

4.3 Vertraulichkeitsklassen

Im Folgenden werden die vier Vertraulichkeitsklassen und die grundlegenden Regeln bezüglich Kennzeichnung, Weitergabe und Absicherung sowie das Schadenspotential bei unsachgemäßem Umgang dargestellt.

„Offen“
Diese Informationen bedürfen keiner Kennzeichnung. Ein Schaden für das Unternehmen kann in keinem Fall entstehen. **Für die Handhabung offener Informationen existieren keine Einschränkungen.**

„Dienstlich“
- Für diese Informationen genügt die implizite Kennzeichnung (siehe 5).
- Sie können intern Mitarbeitern der FMG oder externen Stellen übermittelt werden, soweit die jeweilige Tätigkeit dies mit sich bringt.
- Schaden für das Unternehmen bei einem unsachgemäßen Umgang: gering.

„Vertraulich“

- Für diese Informationen genügt die implizite Kennzeichnung (siehe 5), sofern die Informationen den Kreis der Kernnutzer nicht verlassen.
- Werden sie anderen als Kernnutzern übermittelt, so sind sie vorher explizit als "vertraulich" zu kennzeichnen.
- Sie dürfen nur an bestimmte von dem Informationsverantwortlichen benannte Nutzer übermittelt und von jedem Empfänger nur mit ausdrücklicher Einwilligung des Informationsverantwortlichen an andere Nutzer weitergeleitet werden.
- Externe Dienstleister müssen vor Erhalt der Informationen eine Vertraulichkeitsvereinbarung unterzeichnen.
- Der Verteilerkreis muss auf der ersten Seite genannt werden.
- Schaden für das Unternehmen bei einem unsachgemäßen Umgang: mittel.
- Hinweis: Diese Klasse entspricht im Geheimschutz der Klasse "VS-NUR FÜR DEN DIENSTGEBRAUCH".

„Streng vertraulich“

- Diese Informationen bedürfen stets einer expliziten Kennzeichnung (siehe 5).
- Sie dürfen nur an bestimmte von dem Informationsverantwortlichen benannte Nutzer übermittelt und von jedem Empfänger nur mit ausdrücklicher Einwilligung des Informationsverantwortlichen an andere Nutzer weitergeleitet werden.
- Unabhängig davon ist der Kreis der Nutzer möglichst klein zu halten.
- Externe Dienstleister müssen vor Erhalt der Informationen eine Vertraulichkeitsvereinbarung unterzeichnen.
- Der Verteilerkreis muss auf der ersten Seite genannt werden.
- Schaden für das Unternehmen bei einem unsachgemäßen Umgang: groß bis existenzgefährdend.
- Hinweis : Diese Klasse entspricht im Geheimschutz der Klasse "VS-VERTRAULICH".

Unberührt von dieser Richtlinie bleiben die Sonderfälle der Geheimhaltungsbedürftigkeit gemäß § 79 BetrVG, § 96 SGB IX (Bekanntgabe von Betriebs- und Geschäftsgeheimnissen gegenüber BR, JAV und Schwerbehindertenvertretung).

4.4 Vertraulichkeitsstufe in Abhängigkeit des Lebenszyklus

Eine Information kann verschiedene Stufen an Vertraulichkeit durchlaufen. So können für eine Veröffentlichung vorgesehene Informationen noch als vertraulich einzustufen und zu behandeln sein, solange sie nicht veröffentlicht sind (z. B. Entwurf des Geschäftsberichts). Informationen, die von einem Verfasser aufgezeichnet werden, können ebenfalls einem besonderen Schutz unterliegen (z. B. „Journal“).

4.5 Angebote, Verträge

Angebote und Verträge zu Geschäften über allgemein angebotene Leistungen zu allgemein bekannten Gegenleistungen (z. B. FMG-Raumvermietungen) ohne besondere Nebenabre-

den werden in die Vertraulichkeitsstufe „Dienstlich“ eingestuft. Andere Angebote und Verträge sind je nach Inhalt als „Vertraulich“ oder „Streng vertraulich“ einzustufen. Weitergehende Anforderungen des Vergaberechts usw. bleiben unberührt.

4.6 Informationen von Dritten

Die FMG wahrt die Vertraulichkeit von Kunden- und Lieferanteninformationen und trifft dafür entsprechende Vorkehrungen. Die gesetzlichen und vertraglichen Bestimmungen werden beachtet. Grundsätzlich gelten für Informationen, die der FMG überlassen und mit einer Vertraulichkeitsklasse gekennzeichnet wurden, die gleichen Regelungen wie für FMG-interne Informationen.

5 Kennzeichnung von Informationen

5.1 Explizite Klassifizierung

Sind Informationen explizit als vertraulich oder streng vertraulich zu kennzeichnen, so ist der Träger der Information (z. B. Papierbogen, DVD, E-Mail) deutlich erkennbar mit der Kennzeichnung "vertraulich" bzw. "streng vertraulich" zu versehen. Elektronische Informationen müssen auf der ersten Seite gekennzeichnet werden; nach Möglichkeit sollten alle Seiten gekennzeichnet sein.

Die explizite Kennzeichnung hat immer Vorrang vor der impliziten.

5.2 Implizite Klassifizierung

Die implizite Kennzeichnung stellt eine Erleichterung für die tägliche Arbeit dar. Die Informationen oder Informationsträger sind nicht selbst gekennzeichnet; der Nutzer erkennt die Klassifizierung anhand der Art der Information.

6 Ausdrückliche Verpflichtungserklärungen

Die häufig verwendeten "Non-Disclosure-Agreements" sind nach deutschem Recht nicht unmittelbar zwingend vorgeschrieben, jedoch aus Gründen der Risikovorsorge und mit Blick auf mögliche Schadensersatzforderungen immer in Erwägung zu ziehen. Bei Unklarheiten ist die Konzerneinheit Recht hinzuzuziehen.

Macht ein Geschäftspartner den Informationsaustausch mit der FMG davon abhängig, dass diese ausdrückliche Verschwiegenheits-Verpflichtungserklärungen abgibt, insbesondere nach Formular-Vorgaben des Geschäftspartners, so ist die Konzerneinheit Recht hinzuzuziehen. Keinesfalls sollen ohne vorhergehende Rechtsberatung solche Erklärungen abgegeben werden, die auf die Vereinbarung von Vertragsstrafen, ausländischen Rechts oder unüblicher Gerichtsstände oder auf sonstige für die FMG nachteilige Rechtsfolgen gerichtet sind. Die Konzerneinheit Recht hält für solche Fälle Muster für Verschwiegenheitsvereinbarungen ohne scharfe Rechtsfolgen bereit.

7 Regeln zum Umgang mit Informationen in Papierform

7.1 Ausdruck und Vervielfältigung

„*Dienstlich*“:	Keine Einschränkungen. Wer etwas fotokopiert, ausdruckt oder einscannt, hat Originale und Kopien bzw. Ausdrucke unverzüglich am Gerät abzuholen.
„*Vertraulich*“:	Wie "Dienstlich". Der Vorgang ist darüber hinaus zu beaufsichtigen.
„*Streng Vertraulich*“:	Wie "Dienstlich". Der Vorgang bedarf der Einwilligung des Informationsverantwortlichen und ist zu beaufsichtigen.

7.2 Übermittlung auf dem Postweg

7.2.1 Interne Übermittlung

„*Dienstlich*“:	in unverschlossener Hauspostmappe
„*Vertraulich*“:	in verschlossenem Umschlag
„*Streng vertraulich*“:	doppelter Umschlag: der innere ist mit der Kennzeichnung der Vertraulichkeitsklasse zu versehen, der äußere darf keinen Hinweis auf die Vertraulichkeit enthalten.

7.2.2 Externe Übermittlung

„*Dienstlich*“:	normaler Brief
„*Vertraulich*“:	wie 7.2.1 „*Streng vertraulich*“
„*Streng Vertraulich*“:	wie 7.2.1 „*Streng vertraulich*“, zusätzlich per Einschreiben Übergabe, Kuriersendung, o. ä.

7.3 Übermittlung per Fax

7.3.1 Interne Übermittlung

„*Dienstlich*“:	keine Einschränkungen
„*Vertraulich*“/„*Streng Vertraulich*“:	Deckblatt mit Anzahl der Seiten. Die Sendung ist vom Absender gegenüber dem Empfänger anzukündigen und von diesem abzuwarten, unmittelbar anzunehmen und dem Absender zu bestätigen.

7.3.2 Externe Übermittlung

„Dienstlich“:	Deckblatt mit Anzahl der Seiten
„Vertraulich“:	Deckblatt mit Anzahl der Seiten. Die Sendung ist vom Absender gegenüber dem Empfänger anzukündigen und von diesem abzuwarten, unmittelbar anzunehmen und dem Absender zu bestätigen.
„Streng Vertraulich“:	verboten

7.4 Beseitigung von Informationen in Papierform

„Dienstlich“:	Grundsätzlich genügt die Beseitigung in Papierkörbe am Arbeitsplatz. Personenbezogene Daten müssen gesichert in Einzel-Shreddern oder Shredder-Tonnen vernichtet werden.
„Vertraulich“/„Streng vertraulich“:	gesicherte Beseitigung in Einzel-Shreddern oder Shredder-Tonnen

8 Verbale Weitergabe

„Dienstlich“/„Vertraulich“:	Die Identität des Gesprächspartners ist sicherzustellen *(z. B. Rückruf über Zentrale des Gesprächspartners).* Nur erlaubt, wenn keine Unberechtigten zuhören können (*Vorsicht in S-Bahn, Aufenthaltsräumen etc.)*
„Streng vertraulich“:	Wie *„Dienstlich“/„Vertraulich“*; Streng vertrauliche Informationen dürfen nicht auf Anrufbeantworter / Mailbox hinterlassen werden.

9 Kommunikation nach Außen

Dienstliche, vertrauliche und streng vertrauliche Informationen dürfen an Gesellschafter nur via RC-G kommuniziert werden. Sämtliche sonstigen Anfragen (z. B. Presse) werden von UK oder von UK autorisierten Stellen beantwortet.

10 Regeln zum Umgang mit Informationen in elektronischer Form

10.1 Speicherung von Informationen/Zugriffsrechte

„Dienstlich“/„Vertraulich“:	Die Speicherung muss unter Berücksichtigung der Zugriffsrechte erfolgen, ggf. ist eine explizite Vergabe von Zugriffsrechten notwendig
„Streng vertraulich“:	Die Speicherung muss unter Berücksichtigung der Zugriffsrechte erfolgen, ggf. ist eine explizite Vergabe von Zugriffsrechten notwendig. Die aktuellen Zugriffsrechte sind stetig zu überprüfen, insbesondere bei Zu- oder Abgängen im Kreis der Nutzer.

10.2 Übermittlung per E-Mail

10.2.1 Interne Übermittlung[2]

Alle Klassen: keine Einschränkungen

10.2.2 Externe Übermittlung

„Dienstlich“:	keine Einschränkungen; Anlagen üblicherweise als PDF-Dokument
„Vertraulich“/„Streng Vertraulich“:	Verschlüsselung der E-Mail; Anlagen üblicherweise als PDF-Dokument

10.3 Speicherung auf Mobile Geräte

Mobile Geräte wie Notebooks bedürfen eines besonderen Schutzes.

„Dienstlich“:	keine Einschränkungen
„Vertraulich“/„Streng vertraulich“:	eine Speicherung von Informationen ist nur erlaubt, wenn Verschlüsselungs-Tools eingesetzt werden

10.4 Speicherung auf Mobile Datenträger

Für mobile Datenträger wie CDs, DVDs, USB-Sticks oder mobilen Festplatten gilt folgendes:

„Dienstlich“:	keine Einschränkungen
„Vertraulich“/„Streng vertraulich“:	eine Speicherung von Informationen ist nur erlaubt, wenn Verschlüsselungs-Tools eingesetzt werden. Bei entsprechenden Vorkehrungen (Behandlung wie Papierdokumente, z.B. Wegsperren) kann auf die Verschlüsselung verzichtet werden.

[2] Eine Aufstellung der Domains, die als interne Nutzer gewährtet werden, finden Sie unter http://emotion/home1/fachwissen/unternehmen-prozesse/infosicherheit/infoklass/domains/index.jsp

10.5 Bereitstellung im Internet

Dienstliche, vertrauliche und streng vertrauliche Informationen dürfen nicht im Internet (z. B. Foren, Blogs, Social Networks wie Xing, Facebook oder Twitter) bereitgestellt werden.

10.6 Nutzung von Webdiensten

Dienstliche, vertrauliche und streng vertrauliche Informationen dürfen nur nach dokumentierter Risikoanalyse durch den Informationsverantwortlichen auf Webdiensten abgelegt werden.

10.7 Vernichtung von elektronischen Informationen in Systemen der FMG

Die Vernichtung von elektronischen Informationen erfolgt wie in der jeweiligen Anwendung vorgesehen.

„Dienstlich"/„Vertraulich"/ „Streng vertraulich":	Löschen im Filesystem bzw. normaler Löschvorgang in der Anwendung

10.8 Entsorgung von Informationen auf mobilen Datenträgern

Für mobile Datenträger wie CDs, DVDs, USB-Sticks oder mobilen Festplatten gilt folgendes:

„Dienstlich"/„Vertraulich"/ „Streng vertraulich":	physische Vernichtung des Datenträgers

10.9 Schutz der IT-Systeme

IT-Systeme, insbesondere tragbare (z. B. Notebooks, PDAs und Mobiltelefone) sind vor Diebstahl und Missbrauch zu schützen.

11 Regeln zur physischen Aufbewahrung und Ablage von Informationen

„Dienstlich"/ „Vertraulich"/ „Streng vertraulich":	Unbefugten Zugriff durch Dritte verhindern. Eine der Vertraulichkeitsklasse angemessene Umsetzung ist durch den Informationsverantwortlichen im Einzelfall in Abhängigkeit von den Gefährdungen zu gewährleisten (siehe 10.1,10.2)

11.1 FMG-Campus

„Dienstlich":	Beispiel: Absperren des Büros wo möglich. Bei physisch extra abgesicherten Bereichen sind Sonderregelungen möglich.

„*Vertraulich*“:	Beispiel: Absperren des Büros. Falls gewährleistet ist, dass ausschließlich Kernnutzer (Ausnahme: Feuerwehr, Sicherheitsdienst) Zutritt zum Büro haben, ist diese Maßnahme ausreichend. Ansonsten sind die Informationen bei einer Abwesenheit von mehr als 30 Minuten wegzusperren (z.B. in Schränke, Rollcontainer etc.).
„*Streng vertraulich*“:	Beispiel: Absperren des Büros. Falls gewährleistet ist, dass ausschließlich Kernnutzer (Ausnahme: Feuerwehr, Sicherheitsdienst) Zutritt zum Büro haben, ist diese Maßnahme ausreichend. Ansonsten sind bei einer Abwesenheit von mehr als 5 Minuten die Informationen in sicherer Form wegzusperren (z.B. in Tresor).

Der Informationsverantwortliche kann z.B. für bestimmte Personengruppen wie Hausdamen oder in physisch abgetrennten Bereichen Ausnahmen definieren.

11.2 Unterwegs oder Zuhause

„*Dienstlich*“:/ „*Vertraulich*“:	Beispiel: Aufbewahrung in abgesperrtem Raum, z. B. Hotelzimmer, Heimbüro
„*Streng vertraulich*“:	Vor Zugriff sicher aufbewahren (z. B. Wegsperren in Tresor)

11.3 Besprechungsräume

"Dienstlich"/„*Vertraulich*“/„*Streng vertraulich*“:	Informationen müssen von Weißwandtafeln und Flipcharts entfernt werden, wenn der Raum verlassen wird und Unbefugte (dies können auch FMG-Mitarbeiter sein) ggf. Zugang haben.

12 Versionsverwaltung

Version	Autor	Bemerkungen
1.0	Englert/Cmarits	Ersterstellung
1.01	Englert/Cmarits	Anhang 1 Flyer „Regeln zur Klassifizierung von Informationen“ und Anhang 2 Flyer „Regeln zum Umgang mit Informationen“ entfernt
1.02	Cmarits	Fußnote zum Erkennen von internen Mailadressen geändert
1.03	Cmarits	Anhang „Außerordentlicher Zugriff“ eingefügt; Verantwortlichen auf Deckblatt eingetragen 9.3 Verweis auf Blackberry entfernt
1.1	Cmarits	Außerordentlicher Informationszugriff: Klarstellung bei Zugriff durch Behörden
1.11	Cmarits	Klarstellung Kapitel: • Bereitstellung im Internet Erweiterung um Kapitel: • Kommunikation nach Außen • Nutzung von Webdiensten Außerordentlicher Informationszugriff: Überarbeitung Einleitung beim außerordentlichen Zugriff Rahmenbedingungen bei außerordentlichem Zugriff in Excel ergänzt
1.2	Englert/Cmarits	Kapitel: Kommunikation nach Außen: Anpassung wegen Umorganisation Klarstellungen in den Kapiteln Technischer Sachbearbeiter und Klassifizierung von Informationen
1.3	Englert/Cmarits	Außerordentlicher Informationszugriff: Klarstellung bei der internen Freigabe durch ISM im Abschnitt Anforderer interner Mitarbeiter
1.4	Englert/Cmarits	Außerordentlicher Informationszugriff: Klarstellung bei der Anforderung im Abschnitt Mitarbeiter/Tochter bzw. Mitarbeiter bei externen Kunden
1.5	Englert/Cmarits	Außerordentlicher Informationszugriff: Klarstellung bei der Definition des Begriffes

Version	Autor	Bemerkungen
1.6	Cmarits	Hervorhebungen entfernt,; Schrift auf FMG-Font umgestellt; Fußnote auf interne Mail-Domains angepasst

Anhang 1: Außerordentlicher Informationszugriff

1. Einleitung

Der Zugriff auf Informationen der FMG ist in der vorstehenden „Richtlinie zum Umgang mit Informationen unterschiedlicher Vertraulichkeitsklassen" detailliert beschrieben. In Ausnahmefällen kann es jedoch notwendig sein, Zugriff auf Informationen außerhalb dieser Regelungen zu nehmen. In diesem Fall spricht man von einem „außerordentlichen Zugriff auf Informationen". Dies kann z.B. der Fall sein bei Ermittlungen von Behörden, bei internen Ermittlungen oder aus dringendem betrieblichem Anlass. Kein außerordentlicher Zugriff liegt vor, wenn:

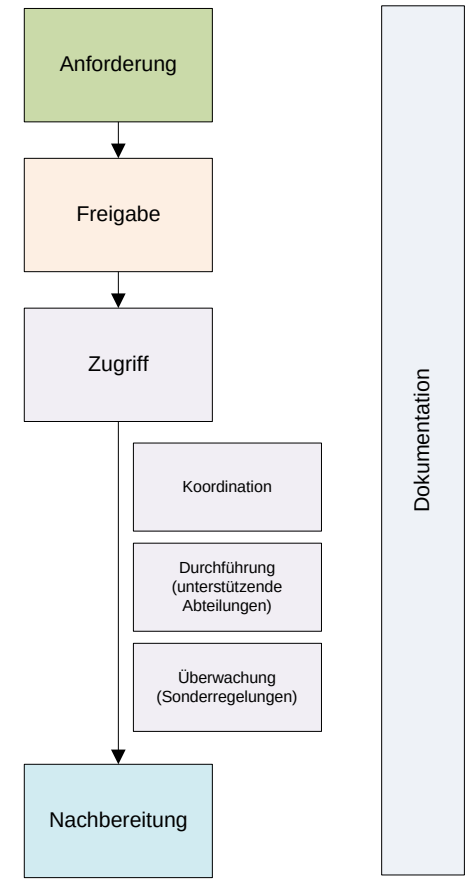
1. Der Anforderer kann selbst auf die Informationen zugreifen
2. Der Anforderer fordert diese beim Informationsverantwortlichen und dieser gibt die Informationen weiter.
3. Der Anforderer fordert die Informationen beim Informationsverantwortlichen an, der auf Grund seiner Berechtigungen Zugriff auf die Informationen hat, diese aber für ihn in aufbereiteter und leichter zugreifbarer Form benötigt (z. B. Erstellung einer CD mit für in besonders selektierten Daten).

Der vorliegende Anhang zur Richtlinie regelt den außerordentlichen Zugriff für den in Kapitel 2 der Richtlinie beschriebenen Geltungsbereich.

Die folgenden Regelungen betreffen nur Informationen der Vertraulichkeitsklassen „dienstlich", „vertraulich" und „streng vertraulich". Informationen der Klasse „offen" sind davon nicht betroffen.

2. Prozess

Der außerordentliche Zugriff auf Informationen erfolgt gemäß folgendem Prozess:



Prozess „Außerordentlicher Zugriff auf Informationen“

Bei der Anwendung dieses Prozesses wird zwischen

- Informationen in IT-Systemen (z.B. E-Mails, Dateien, Datenbanken, Protokolldaten zu Internet, E-Mail, Geschäftstelefon, Geschäftshandy, Blackberry) und
- sonstigen Informationen (z.B. in Papierform, auf lokalem Datenträger wie DVD)

unterschieden.

Die detaillierte Ausgestaltung des Prozesses unterscheidet nach Informationsart und Anforderer. Die damit verbundenen Regelungen sind in der nachfolgenden Tabelle „Verfahren außerordentlicher Informationszugriff“ ersichtlich. Das gesamte Verfahren wird dokumentiert gemäß der Vorlage „Dokumentation außerordentlicher Informationszugriff“.

2.1 Anforderung

Der Prozess zum außerordentlichen Zugriff auf Informationen wird durch eine Anforderung ausgelöst. Fordern andere – bis dato nicht definierte Stellen – einen außerordentlichen Zugriff an, so hat sich dieser Anforderer an den Beauftragten für Informationssicherheit des FMG-Konzerns zu wenden.

Insbesondere ist darauf zu achten, dass nur der für den jeweiligen Fall notwendige Informationsbestand angefordert wird. Eine pauschale Anforderung („alle Informationen die damit zu tun haben könnten") ist ausgeschlossen.

2.2 Freigabe

Für einen außerordentlichen Zugriff ist zwingend die Freigabe der definierten Stellen (siehe nachfolgende Tabelle) notwendig.

2.3. Zugriff

Der Zugriff auf die Informationen wird durch die definierten Stellen koordiniert. Für den eigentlichen Zugriff auf die Informationen ist zumeist die Unterstützung von Experten aus Fachabteilungen oder von Dienstleistern notwendig. In speziellen Fällen (Zugriff auf personenbezogene oder private Informationen) sind Sonderregelungen in Kraft, die den Zugriff durch definierte Stellen festlegen.

2.4 Nachbereitung

Zur Aufbereitung und Konsolidierung ist jeder außerordentliche Zugriff auf Informationen (ab Anforderung!) dem Beauftragtem für Informationssicherheit des FMG-Konzerns zu melden.

3. Verfahren außerordentlicher Informationszugriff

3. Verfahren außerordentlicher Informationszugriff

Stand: V1.5 vom 03. April 2012

		Informationen in IT-Systemen (z.B. E-Mails, Dateien, Datenbanken, Protokolldaten zu Internet, E-Mail, Geschäftstelefon, Geschäftshandy, Blackberry)					Sonstige Informationen (z.B. bereits existent in Papierform, auf lokalem Datenträger wie DVD, ..)				
Anforderung	Anforderer	Revision, Wirtschaftsprüfung	Mitarbeiter interner Bereiche	Mitarbeiter Tochter (für Systeme, die bei der FMG beauftragt wurden)	Kunden / sonstigen Dritten (für Systeme, die bei der FMG beauftragt wurden)	Ermittlungsbehörden / RCJ	Revision, Wirtschaftsprüfung	Interne Bereiche	Mitarbeiter Tochter nicht relevant für FMG	Mitarbeiter bei externen Kunden / sonstigen Dritten nicht relevant für FMG	Ermittlungsbehörden
	Art der Information			Anforderung von beim IT-Dienstleister gespeicherten Daten	Anforderung von beim IT-Dienstleister gespeicherten Daten						
	Genehmigung auf Anforderer-Seite	Interne Revision, Externe Revision, Wirtschaftsprüfer	FK1/FK2, Info-Verantwortlicher	Geschäftsführer Tochter	Geschäftsführer (bei externe Kunden / sonstigen Dritten)	Staatsanwaltschaft, Polizei, andere Hilfsbeamte der Staatsanwaltschaft	Interne Revision	Vorgesetzter (min. FK2), Info-Verantwortlicher			Staatsanwaltschaft, Polizei
Freigabe	FMG interne-Freigabe	Generelle Freigabe durch GF ist erteilt	ISM (sofern der Informationsverantwortliche keinen Zugriff auf die Informationen besitzt) (evtl. zusätzliche Freigabe Infoverantwortlichen der angeforderten Daten) - bei personenbezogenen Daten ist die Freigabe durch ISM nicht notwendig (s. Sonderregelung personenbezogene Daten)	Falls IT involviert: Freigabe durch MOD, sonst nicht benötigt	Falls IT involviert: Freigabe durch MOD, sonst nicht benötigt	RCJ (bei Nichtverfügbarkeit SE-Führungsbereitschaft)	Generelle Freigabe durch GF ist erteilt	ISM (evtl. zusätzliche Freigabe Infoverantwortlichen der angeforderten Daten)			RCJ (bei Nichtverfügbarkeit SE-Führungsbereitschaft)
	Sonderregelung personenbezogene Daten (auch dann anzuwenden, wenn personenbezogene Daten nicht angefordert, aber mit anderen Daten zusammen gespeichert sind - z.B. Internet-Protokolle)	Freigabe durch DSB notwendig	zusätzlich Freigabe durch DSB und BR der FMG GmbH notwendig	keine	keine	keine	keine	zusätzlich Freigabe durch DSB und BR der FMG GmbH notwendig			keine
	Sonderregelung, bei IT-System mit genehmigter Privatnutzung (derzeit nur Geschäftstelefon, DELFIN Fundgrube etc., Duo-Bill bei Telefonverbindungsdaten) (auch dann anzuwenden, wenn private Daten nicht angefordert, aber mit anderen Daten zusammen gespeichert sind)	keine	zusätzlich Freigabe durch DSB	keine	keine	keine	keine	zusätzlich Freigabe durch DSB			keine
	Bemerkung										
Zugriff	Koordination	RSR (bei Revision); FMG-Fachabteilung bei Wirtschaftsprüfung	ISM (bei personenbezogenen Daten DSB möglich)	ISM	IT-Dienstleister	RCJ (bei Nichtverfügbarkeit SE-Führungsbereitschaft)	RSR (bei Revision); FMG-Fachabteilung bei Wirtschaftsprüfung	ISM (bei personenbezogenen daten auch DSB möglich)			RCJ (bei Nichtverfügbarkeit SE-Führungsbereitschaft)
	Sonderregelung personenbezogene Daten (auch dann anzuwenden, wenn personenbezogene Daten nicht angefordert, aber mit anderen Daten zusammen gespeichert sind - z.B. Internet-Protokolle)		Teilnahme DSB FMG GmbH notwendig und BR (falls BR Teilnahme erforderlich sieht). 4-Augenprinzip muss gewährleistet sein	keine	keine	Auswertung nach dem Vier-Augen-Prinzip (anfordernde Behörde + FMG) - (Berücksichtigung BR erforderlich!)	keine	Teilnahme DSB FMG GmbH notwendig und BR (falls BR Teilnahme erforderlich sieht). 4-Augenprinzip muss gewährleistet sein			keine
	System mit genehmigter Privatnutzung (derzeit nur Geschäftstelefon, DELFIN Fundgrube etc., Duo-Bill bei Telefonverbindungsdaten) (auch dann anzuwenden, wenn private Daten nicht		Teilnahme DSB FMG GmbH nach dessen Entscheidung 4-Augenprinzip muss gewährleistet sein	keine	keine	keine		Teilnahme DSB FMG GmbH nach dessen Entscheidung 4-Augenprinzip muss gewährleistet sein			keine
	Mögliche unterstützende Abteilung(en)	IT, SE, PE, TE + geprüfter Bereich	IT, SE, TE, PE	IT, SE, TE, PE	IT, SE, TE, PE	IT, SE, TE, PE	SE, PE + geprüfter Bereich	IT, SE, TE, PE			SE, PE
	Unverzüglich Info an		ISM, falls Freigabe durch DSB erfolgt ist		ISM	ISM	ISM	ISM			ISM
	Bereichsspezifische Zusatzregeln	IT: unverzügliche Information des MOD	IT: unverzügliche Information des MOD			IT: unverzügliche Information des MOD	IT: unverzügliche Information des MOD	IT: unverzügliche Information des MOD			IT: unverzügliche Information des MOD
	Rahmenbedingungen					Aushändigung von Datenträgern nur mit richterlichem Beschluß. Forensisches Duplikat verbleibt bei ISM					

Abkürzungen:

ISM	Beauftragter für Informationssicherheit des FMG-Konzerns
DSB	Datenschutzbeauftragter
BR	Betriebsrat
MOD	Manager on Duty im Servicebereich IT (mindestens FK2)